LEGIBILITY NOTICE

A major purpose of the Technical Information Center is to provide the broadest dissemination possible of information contained in DOE's Research and Development Reports to business, industry, the academic community, and federal, state and local governments.

Although a small portion of this report is not reproducible, it is being made available to expedite the availability of information on the research discussed herein.

LA-UR -89-2130

Los Alamos National Laboratory is operated by the University of California for the United States Department of Energy under contract W-7405-ENG-36

LA-UR--89-2130

DE89 014221

TITLE **LOS ALAMOS CENTER FOR COMPUTER SECURITY FORMAL COMPUTER SECURITY MODEL**

AUTHOR(S) J. S. Dreicer and W. J. Hunteman

SUBMITTED TO 30th Annual Meeting of the Institute of Nuclear Materials Management, Orlando, July 9-12, 1989

DISCLAIMER

Los Alamos
DOE Center for Computer Security
Los Alamos National Laboratory
Los Alamos, New Mexico 87545

LOS ALAMOS CCS FORMAL COMPUTER SECURITY MODEL*

Jared S. Dreicer, William J. Hunteman, and J. T. Markin
Los Alamos National Laboratory
Los Alamos, New Mexico 87545

ABSTRACT

This paper provides a brief presentation of the formal computer security model currently being developed at the Los Alamos Department of Energy (DOE) Center for Computer Security (CCS). The need to test and verify DOE computer security policy implementation first motivated this effort. The actual analytical model was a result of the integration of current research in computer security and previous modeling and research experiences. The model is being developed to define a generic view of the computer and network security domains, to provide a theoretical basis for the design of a security model, and to address the limitations of present formal mathematical models for computer security. The fundamental objective of computer security is to prevent the unauthorized and unaccountable access to a system. The inherent vulnerabilities of computer systems result in various threats from unauthorized access. The foundation of the Los Alamos DOE CCS model is a series of functionally dependent probability equations, relations, and expressions. The model is undergoing continued discrimination and evolution. We expect to apply the model to the discipline of the Bell & LaPadula abstract sets of objects and subjects.

INTRODUCTION

This paper has three goals: (1) to introduce the Los Alamos Center for Computer Security CCS (LACCS) model, (2) to briefly introduce and discuss computer security, and (3) to discuss the future direction and application of this work.

*This work is supported by the U.S. Department of Energy, Office of Safeguards and Security, Computer and Technical Security Branch.

Other formal models have been developed; two of the most prominent are the Bell & LaPadula and the SRI International models. Both of these models have undergone scrutiny and analysis for years, and it is generally agreed that they are adequate for the development of a secure system.[1,2] Furthermore, both the Bell & LaPadula and the SRI International models have provided insight into the development of multilevel secure systems. The LACCS model attempts to alleviate the limitations of these other models.

Application of the formal models to securing a computer system requires consideration of all aspects of computer security. These aspects include the traditional hardware and software, as well as the operating environment of the computer system.

COMPUTER SECURITY

The fundamental objective of securing a computer system is to prevent or deter unauthorized or unaccountable access to the system and the information being processed or stored (very similar to safeguarding nuclear material). This objective requires a holistic approach to security that goes beyond the traditional hardware and software views of computer security. The vulnerabilities in the computer system hardware and software have received the most attention in previous research that focused on evaluating the likelihood that a given threat would successfully exploit hardware or software vulnerabilities.

However, the operating environment for the system provides a larger, and possibly easier to exploit, range of vulnerabilities. The threat agent's goal is to achieve unauthorized disclosure, modification, or destruction of information or hardware regardless of where the vulnerability exists. The LACCS model provides an integrated view of the system and its operating environment. The model supports a global view of the system while addressing the threat agent's perspective.

The total environment of a secure computing system often receives relatively little attention when one considers threats against the information. Vulnerabilities in the operating environment (procedural issues) can contribute to vulnerabilities in some of the system security mechanisms. Extreme situations have been observed

where a breakdown in the procedures has negated many of the information protection mechanisms.

Another avenue of system attack for the threat agent is to deny authorized use of the computing system. Use can be denied through a variety of techniques. The introduction of faulty circuit boards or microcode can deny use and perhaps physically damage a system. Software actions, including introducing a virus, can cause a system to frustrate or not respond to its users with the resultant effect that the system is not used in an effective manner.

Use of the system can also be denied through a variety of techniques that do not require access to the system hardware or software. The introduction of commonly available chemicals into the heating and ventilation system for the computer facility can result in the shutdown and evacuation of the entire facility. Frequent false alarms, e.g., bomb threats and fire alarms, can also deny use of the system.

Threats resulting in the disclosure, modification, or destruction of information can be achieved through a wide variety of operations specific to the information sensitivity and the computing system being attacked. However, most of these actions are accomplished through problems or difficulties in information management and the authorization, enforcement, and verification methodologies employed in the system.[3] Some specific DOE areas affected by the methodologies are

- user authentication and authorization, e.g., personnel clearances, physical access controls, and software mechanisms for authentication and authorization;

- information management, e.g., configuration management of hardware and software, discretionary and mandatory access controls, backup of sensitive information, accountability, marking of objects, and assurance testing;

- communications, e.g., construction of secure communications facilities; and

- operating procedures, e.g., clearing and sanitization of storage objects and reliable marking of human readable output.

Previous work in computer security models, e.g., Bell & LaPadula,[4] and other research have concentrated on authorization and classification levels of information and information management. These models have not incorporated the issues involved in defining the necessary secure environment for the system. The LACCS model provides a comprehensive framework for considering all computer security issues.

LACCS MODEL

In an analytical manner, the LACCS model incorporates the computer security concerns and issues briefly discussed in the introduction and the previous section. Further, the LACCS model goes beyond simply characterizing the DOE computer security policy; it addresses generic problems of computer security.

A generic model is required to support the capability to consider "what-if" questions in the computer security and network domain. This is necessary because of the speed and frequency of technological change in computer science research and the computer industry (hardware and software).[5] New computer system configurations and topologies, communication and design protocols, threats, vulnerabilities, and operating methodologies are continuously developed and used. The ability to employ these technological developments or counter them depends on the capability to determine their operational effectiveness.

Applying the LACCS model to subjects and objects in terms of the Bell & LaPadula model definition essentially requires mapping these abstract sets to the equivalent abstraction in the LACCS model. However, the perspective of the Bell & LaPadula model is fundamentally different, in that it indicates whether or not the system state is secure. The comprehensive system state is determined by the combination of all transition states. If each transition state is secure, then the resulting system state is secure; this is known as the Basic Security Theorem.[6] Security is defined in terms of the relationship between the clearances of subjects and the classification of system objects. As long as the rules and dominance relation with respect to access control and management are observed, security is maintained.

For the LACCS model, two perspectives are associated with security: the attacker's (insider, agent, and hacker) and the defender's (computer system security officer). In terms of subjects and objects, the attacker and defender, as well as the functioning computer system, are all subjects (active entities), and the information resident on the computer system is an object (passive entity).

The following probability equations and relations abstractly describe the essential subsystem and interface components from the standpoint of the two security perspectives and from a physical computer and network systems outlook. Equation (1) results in a measure of the security expectancy (S_e) for the modeled system: the defender's ultimate consideration.

$$S_e = 1.0 - D_e \tag{1}$$

Equation (1) is defined in terms of subjects and objects, since damage expectancy (D_e) is composed of both active and passive entities. The security expectancy measure is the comprehensive result of the model. The security expectancy (S_e) and the damage expectancy (D_e) for a system are inversely related.

Designers of a system are concerned with the security expectancy for actual or proposed systems. Both system security developers and attackers are interested in the damage expectancy for the systems, but for distinctly different reasons. Damage expectancy is determined by threat arrival, which is a concern for security developers and attackers, and threat damage, which is a concern for system designers. Damage expectancy is principally related to subjects, but the subjects have objects as components, indicated in the following discussion. Equation (2) demonstrates the relation.

$$D_e = F(T_{ad}, T_d, T_{aa}) \tag{2}$$

Threat arrival for defender (T_{ad}) is related to the penetrability, resistivity, and discrimination reliability of the system to the

entrance of a threat element. The remaining components, threat damage (T_d) and arrival of attacker threat (T_{aa}), are discussed below. Equation (3) depicts the factors that affect the threat arrival.

$$T_{ad} = F(T_{sps}, S_{pts}, S_r) \quad (3)$$

T_{sps} is the survivability of the penetrating threat, an active subject, before entering the system. S_{pts}, a subject, is the pre-threat survivability of the system. S_r is the system reliability, a subject. These factors are dependent upon the threat access mechanism and implementation and the system integrity.

Threat damage (T_d) is dependent on the system's vulnerabilities, information sensitivity, mission criticality, and resilience to disclosure and deterioration. These components are represented in Equation (4).

$$T_d = F(V_n, I_c, M_c, S_{rdi}, S_{rdt}) \quad (4)$$

V_n is the vulnerability or hardness of the system: this is an object. I_c is the highest classification of information resident on the system: this is an object. M_c is a measure of the national importance of the system: this is an object. S_{rdi} and S_{rdt} are indicators of the capacity of the system to limit information exposure and recover from deterioration. These factors result from the integration of subjects and objects.

Threat arrival for attacker (T_{aa}) is determined by the penetration initiation, success, and potential. Equation (5) presents the relation.

$$T_{aa} = F(T_{atp}, T_{p/a}, T_{h/a}) \quad (5)$$

T_{atp} is a threat attempt: a subject. $T_{p/a}$ is a threat penetration given an attempt: a subject. $T_{h/a}$ is the harm that results from a successful penetration attempt. These components depend on the threat prevention and access mechanisms and the type of methodology and implementation. The interpretation of T_{aa} can range from representing a system that has been destroyed ($T_{aa} = 1.0$) to one that has been harmed ($0.0 < T_{aa} < 1.0$).

CONCLUSIONS

The LACCS model was recently formulated and is in the process of examination and refinement. The model has undergone several modifications to better conform to the computer and network domain. The authors intend to use the model as a top-level definition of a secure system. Further work will identify the similarities and differences between the Bell & LaPadula objects and subjects and the LACCS model terminology. Additional work is planned to apply the LACCS model to the development and review of secure systems and networks. Due to the generic nature of the model, application to other fields is possible; in particular, nuclear safeguards appears to be a prime candidate.

REFERENCES

1. C. Landwehr, "Formal Models for Computer Security," ACM Computing Surveys 13(3), 247-278 (September 1981).

2. T. Taylor, "Comparison Paper Between The Bell and LaPadula Model and The SRI Model," Proceedings of the 1984 Symposium on Security and Privacy (IEEE Computer Society Press, Silver Spring, Maryland, 1984), pp. 195-202

3. J. Tape, C. Coulter, J. Markin, K. Thomas, "Integrated Safeguards and Faciltiy Design and Operations," Los Alamos National Laboratory document LA-UR-8879 (November 1987).

4. D. Bell and L. LaPadula, "Secure Computer Systems: Mathematical Foundations and Model," Mitre Corp. report M74-244 (1973).

5. C. Landwehr, "The Best Available Technologies for Computer Security," IEEE Computer, 86-100 (July 1983).

6. Department of Defense Trusted Computer System Evaluation Criteria, DoD 5200.28-STD (December 1985).